# INFORMED POSITIONAL EMBEDDING FOR MULTI-BIT WATERMARKING

*Paulo Vinicius Koerich Borges and Joceli Mayer*

LPDS: Digital Signal Processing Laboratory
Department of Electrical Engineering
Federal University of Santa Catarina, UFSC, SC, Brazil
{paulo,mayer}@eel.ufsc.br

## ABSTRACT

In this work, we propose an informed positional coding scheme by extending the position based watermarking approach [5]. In contrast to the traditional watermarking approaches where the information is carried by the watermark itself, in the proposed positional approach, the information is related to the *position* of the embedded watermarks in the image. Moreover, we propose an optimization criteria to select the best among a few available positions to embed a watermark to represent an information and also the best watermark from a codebook of watermarks. Results illustrate the better robustness and transparency performance when compared to the traditional spread spectrum techniques. Moreover, we show that the method presents better robustness to collusion attacks, as illustrated by experiments.

## 1. INTRODUCTION

This work proposes on a novel approach to watermarking, coined position based watermarking (PBW). In contrast to other methods, we are able to select the watermark to be embedded from a codebook of watermarks and also to choose which regions in the image will receive the selected watermark. The novel approach is able to further improve the perceptual transparency for a given robustness as compared to traditional methods.

In Section 2 we present an overview of the PBW, in Section 3 we propose improvements to the PBW and provide some analysis of their properties. In Section 4, we investigate the method robustness to the collusion attacks and compare against the traditional spread spectrum approach. Section 5 provides results and discussions and also comparisons to the traditional spread-spectrum (SS) approach.

This work was supported by CNPq, Grants Nos. 55164/01-1 and 550658/02-5.

## 2. OVERVIEW OF PBW

In traditional watermarking schemes, the information to be transmitted is usually related to the watermark sequence itself. In PBW, the embedding procedure is based on the position of pseudo-random watermark blocks. The blocks are inserted in the image and their position correspond to the information to be transmitted.

Let us consider a host image pixel grid of size $M \times N$, where $M$ is the image height and $N$ is the image width. Assume we add to this grid $K$ watermarks $w$ of size $w_h \times w_w$. Each watermark consists of 1's and -1's, with equal probability, modulated by a gain $\alpha$. Let $Ref$ be the pixel $(0, 0)$ of the watermark block (Fig. 1).

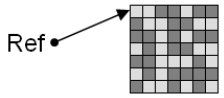


**Fig. 1**. Representation of the reference pixel.

Assume we want to embed the following bit string to the image: $S_1 = 0010011$. By using an appropriate coding scheme, $S_1$ can be represented, for instance, by the embedding of one watermark $w$ with its reference $Ref$ placed over pixel $(10, 25)$ of the host image and another watermark $w$ with its reference $Ref$ over pixel $(75, 120)$ of the host image.

Considering traditional additive embedding technique in the spatial domain, the marked image is identical to the original one, except where the watermark blocks are placed. The detector scans the image and finds the positions in the image presenting the highest correlation to the watermark blocks, as illustrated in Fig. 2. These positions are finally decoded to the bit string they represent.

The capacity of the proposed method depends on the image size and on the quantity and size of watermark blocks. Avoiding superposition of watermarks and considering that splitting of the watermark is not permitted, the capacity [5] is expressed by:

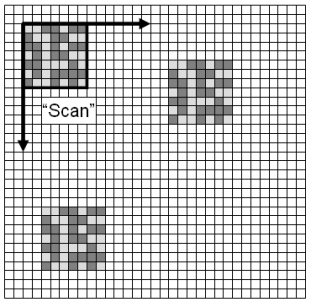


**Fig. 2**. The process of searching for a watermark block.

$$Cap = \frac{\log[C(p,K)]}{\log 2} = \log_2[C(p,K)] \quad (1)$$

where

$$C(p,K) = \frac{p!}{(p-K)!K!} \quad (2)$$

and

$$p = (N-w+1)^2 - (K-1)[(2w-1)^2 - 1] \quad (3)$$

is the number of available positions for the insertion of $K$ watermarks. Making use of $K = 2$, watermark blocks of size $32 \times 32$, we have a capacity of 30 bits for a $256 \times 256$ ($N = 256$) image.

## 3. PROPOSED IMPROVEMENTS

### 3.1. The detection procedure

One major disadvantage of the proposed PBW in [5] is the computational complexity of the detection process. The operation of scanning the image and calculating the correlation for each position can be very time consuming for large images. As a simple alternative to overcome this inefficiency, we employ the *correlation theorem* to carry out the detection in the frequency domain. A straightforward analysis [4] indicates that the detection in the frequency domain requires $3MN\log_2(MN)$ operations, while in the spatial domain, the same task requires $2MN(w_h \cdot w_w)$ operations.

For watermark blocks of medium and large sizes, detection in the frequency domain becomes much faster than in spatial domain.

### 3.2. Optimization Process

The coding scheme proposed in [5] consists of an one-to-many mapping to code an information bit string $S$ to $K$ positions $s_j$ $(j = 1, 2, ..., K)$ in the image. It is suggested that instead of having only one single set $Q$ of positions representing $S$, we propose the use of more sets. Thus, we have $q$ sets $Q_i$ $(i = 1, 2, ..., q)$ of positions to choose to insert the $K$ watermarks when embedding $S$. In Fig. 3 we illustrate these sets, for $K = 2$ and $q = 5$. A metric based on information entropy is suggested in [4] to estimate a suitable value for $q$.

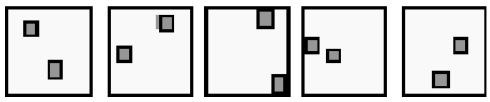

**Fig. 3**. Illustration of different position watermark sets representing the same bit string for $q = 5$ and $K = 2$.

Thus, we can choose the best $Q_i$ from $q$ sets based on the objective or perceptual fidelity and detection performance for the application at hand. We employ the Pareto optimization method [6] to find the best set for a given fidelity versus robustness trade-off. Details of the optimization process are given in [4].

### 3.3. Selecting the best watermark from a codebook

Since PBW does not need to encode the information into the watermark, we are able to design a codebook of watermarks in order to improve the detection performance by choosing the best available watermark to embed in a particular image. The best watermark will have the least correlation to the host image, when compared to other watermark candidates. Moreover, the probability of finding a proper watermark regarding detection in a larger codebook is better. Fig. 4 illustrates how the detection performance improves as the quantity of available watermarks increases.

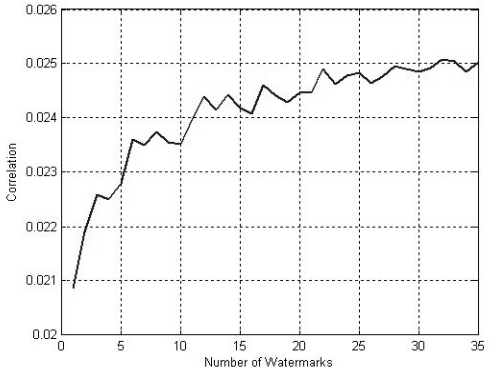


**Fig. 4**. Influence of the number of available watermarks in the detection value.

## 4. ROBUSTNESS TO COLLUSION ATTACKS

Fingerprinting is one of the important applications for watermarking systems [3], in which illegal copies of a Work

can be traced. Collusion attacks raise an interesting security issue [3] for fingerprinting applications. In this attack, $C$ colluded users, each with a different watermarked version of the same Work, average their $C$ watermarked versions of the Work, resulting in the reduction of the watermark energy. As a result, depending on how many copies $C$ were available, the watermark may become undetectable, and the resulting colluded Work has a better fidelity to the original when compared to one of the watermarked copies.

In this context, we show that PBW, due to its distinguished approach, can be set to be more resilient to collusion attacks in fingerprinting applications, when compared with spread spectrum techniques [1]. PBW does not modify the whole image, but only small parts of it. Furthermore, for the same image, different users tend to have signatures watermarked in different regions of the image with high probability, considering that $w_h w_w \ll MN$.

Consider $I_0$ as a vector of length $MN$ containing the elements of the host image. An antipodal multi-bit message $B$ of length $L$ is to be embedded into $I_0$.

$$B = [b_1, b_2, \ldots, b_L], b_l \in \{-1, +1\} \tag{4}$$

In the case of SS watermarking, to obtain a watermark vector $W$ of length $MN$ carrying the $L$-bit message, a set $\mathcal{P}$ of $L$ reference marks is created. Each reference mark $P_l$ is a pseudo-random sequence of length $MN$, with zero average.

$$\mathcal{P} = \{P_1, P_2, \ldots, P_L\} \tag{5}$$

$$P_l = [p_{l1}, p_{l2}, \ldots, p_{lM \cdot N}], p_{li} \in \{-1, +1\} \tag{6}$$

where pseudo-random sequence elements $p_{li}$ are random numbers assuming -1 or +1 with equal probability.

The $L$-bit message $B$ is spread into a $M \cdot N$-dimensional sequence $W$ corresponding to the watermark vector, multiplied by a gain factor $\alpha$:

$$W = \alpha \sum_{l=1}^{L} b_l P_l \tag{7}$$

The watermarked image vector $I_W$ is finally obtained from:

$$I_W = I_0 + W \tag{8}$$

Considering the use of correlation to detect the watermark, a decision variable $D_l$ is given by:

$$D_l = \langle P_l, I_W \rangle = \frac{1}{MN} \sum_{i=1}^{MN} p_{li} \cdot I_{W_i} \tag{9}$$

in which $l$ represents the pseudo-random sequence index and $i$ represents the vector element index.

Let $I_{Col}$ be an attacked (by collusion) version of $I_W$:

$$I_{Col} = \frac{1}{C} \sum_{j=1}^{C} I_0 + \frac{1}{C} \sum_{j=1}^{C} W_j \tag{10}$$

where $W_j$ is the watermark embedded into the $j$-th colluded image. Considering a collusion attack, from equation (9):

$$\begin{aligned} D_l &= \langle P_l, I_{Col} \rangle \\ &= \langle P_l, \frac{1}{C} \Big( \sum_{j=1}^{C} I_0 + \sum_{j=1}^{C} W_j \Big) \rangle \\ &= \langle P_l, \Big[ I_0 + \frac{1}{C} \sum_{j=1, j \neq J}^{C} W_j + \frac{1}{C} \cdot W_J \Big] \rangle \end{aligned} \tag{11}$$

in which $J$ is a constant and $W_J$ was generated using $P_l$. Note that in this application of fingerprinting, each different user has a different set $\mathcal{P}$. Expanding (11):

$$\begin{aligned} D_l = \langle P_l, I_0 \rangle + & \quad \text{( A)} \\ \langle P_l, \frac{1}{C} \sum_{j=1, j \neq J}^{C} W_j) \rangle + & \quad \text{(B)} \\ \langle P_l, \frac{1}{C} W_J \rangle & \quad \text{( C)} \end{aligned} \tag{12}$$

Regarding (A):

For SS, A = constant.

For PBW, A = $\min\{\langle P_t, I_0 \rangle\}$, $t = 1, 2, \ldots, T$, where $P_t$ is a watermark block from the watermark codebook (Subsection 3.3).

Regarding (B):

For PBW, the term B has a high probability $Pr$ (defined later) of being equal to zero .

For SS, B>0, due to the interference among the $C \cdot L$ sequences.

Regarding (C):

In this term, usually occurs interference among the $L$ sequences that form the watermark $W$ in the SS technique. In PBW, we have no interference, since $W_J = P_l$.

In PBW, when $w_h \cdot w_w \ll M \cdot N$, there is a high probability $Pr$ of not ocurring superposition of watermark blocks in the collusion process, case in which we achieve B = 0 in equation (12). Specifically, from a geometric analysis, we find that colluding $C$ images, $Pr$ is given by:

$$Pr = 1 - K^2 \cdot \frac{(2 \cdot w_h - 1) \cdot (2 \cdot w_w - 1)}{M \times N} \cdot (C - 1) \tag{13}$$

**Table 1**. Fidelity Comparison: Watson Perceptual Model$^{\diamond}$ SNR$^{\bigstar}$

| Amount of Distortion | | |
|---|---|---|
| **Image** | Informed PBW | Spread Spectrum |
| Lena | $0.0018^{\diamond}$ $54.01^{\bigstar}$ | $0.0249^{\diamond}$ $38.44^{\bigstar}$ |
| **AVERAGE** | $0.00175^{\diamond}$ $53.80^{\bigstar}$ | $0.0301^{\diamond}$ $39.02^{\bigstar}$ |

## 5. EXPERIMENTS

Although PBW can be applied in any domain (spatial, frequency, wavelet) and also for other media like audio and video, here we present a comparison with the existing SS [1] method in the spatial domain. It should be noted that many of the tools (pre-filtering, masking, etc) that can be used in SS watermarking can be used for PBW as well.

In the experiment, for a fair comparison, we tune both techniques (informed PBW and SS) to the same capacity (28 bits) and fix a gain $\alpha$ just strong enough to assure $100\%$ successful detection in the 250 test images. We used images of size $256 \times 256$, $K = 2$, and watermark block of size $32 \times 32$. Having assigned these parameters, we tested the systems' fidelity. From the results of Table 1 we note that informed PBW does offer both a higher SNR and a higher measure according to Watson's perceptual model [2]. The AVERAGE field represents the average of results for 250 tested images. Fig. 6 shows the watermarked image of Lena in this experiment, presenting a high perceptual quality. Results for the blind embedding PBW can be found in [5].

In Figure 5 we compare SS and PBW regarding robustness to collusion attacks. The horizontal axis indicates the tested image. The vertical represents the number $C$ of images included in the attack. The marks indicate the maximum value of $C$ for which the systems present a perfect detection. A superior performance of the PBW method is noted, in agreement with the analysis of Section 4.

Regarding robustness, experiments illustrated that PBW is more robust to AWGN attacks than SS, when both methods are tuned to the same fidelity by adjusting the $\alpha$ factor and we embed 28 bits for both techniques.

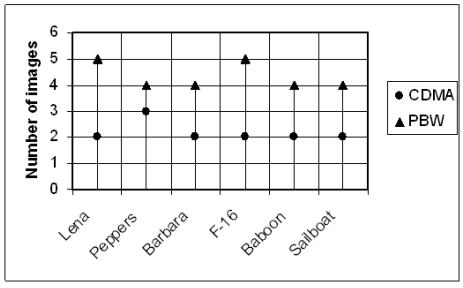


**Fig. 5**. Comparison between SS$^{\bullet}$ (CDMA) and PBW$^{\blacktriangle}$, regarding robustness to collusion attacks.

**Fig. 6**. Lena watermarked with 28 bits, using PBW.

## 6. CONCLUSIONS

In this paper, we have proposed an informed insertion method for the novel PBW technique. We have introduced an optimization criteria to select the best positions to embed the watermarks. Results illustrate that PBW has a better performance than SS, regarding fidelity and robustness to AWGN. Also, we analyzed and illustrated with experiments that PBW can be more robust to collusion attacks.

## 7. REFERENCES


[1] Ingemar J. Cox, Matthew L. Miller and Jeffrey A. Bloom, *Digital Watermarking*, Morgan Kaufmann, 2002.

[2] A. B. Watson, "DCT quantization matrices optimized for individual images," *Human Vision, Visual Processing, and Digital Display IV*, SPIE 1913:202-216, 1993.

[3] M.Wu, W. Trappe, Z. Wang, and K.J. Ray Liu, "Collusion-resistant fingerprinting for multimedia," *IEEE Signal Processing Magazine*, vol. 21, no. 2, pp. 15-27, March 2004.

[4] P.V. Borges "Positional Model for Digital Watermarks", *Master Thesis in Electrical Engineering* - Federal University of Santa Catarina - Brazil - 2004.

[5] P. V. K. Borges and J. Mayer, "Position Based Watermarking" *IEEE Proc. of 3rd Int'l Symposium on Image and Signal Proc. and Analysis - ISPA*, 2003.

[6] Winston, Wayne L., *Introduction to Mathematical Programming: applications and algorithms*, Duxbury Press, 1995.

[7] T. M. Cover, J. A. Thomas. *Elements of Information Theory*. New York: John Wiley & Sons, 1991.